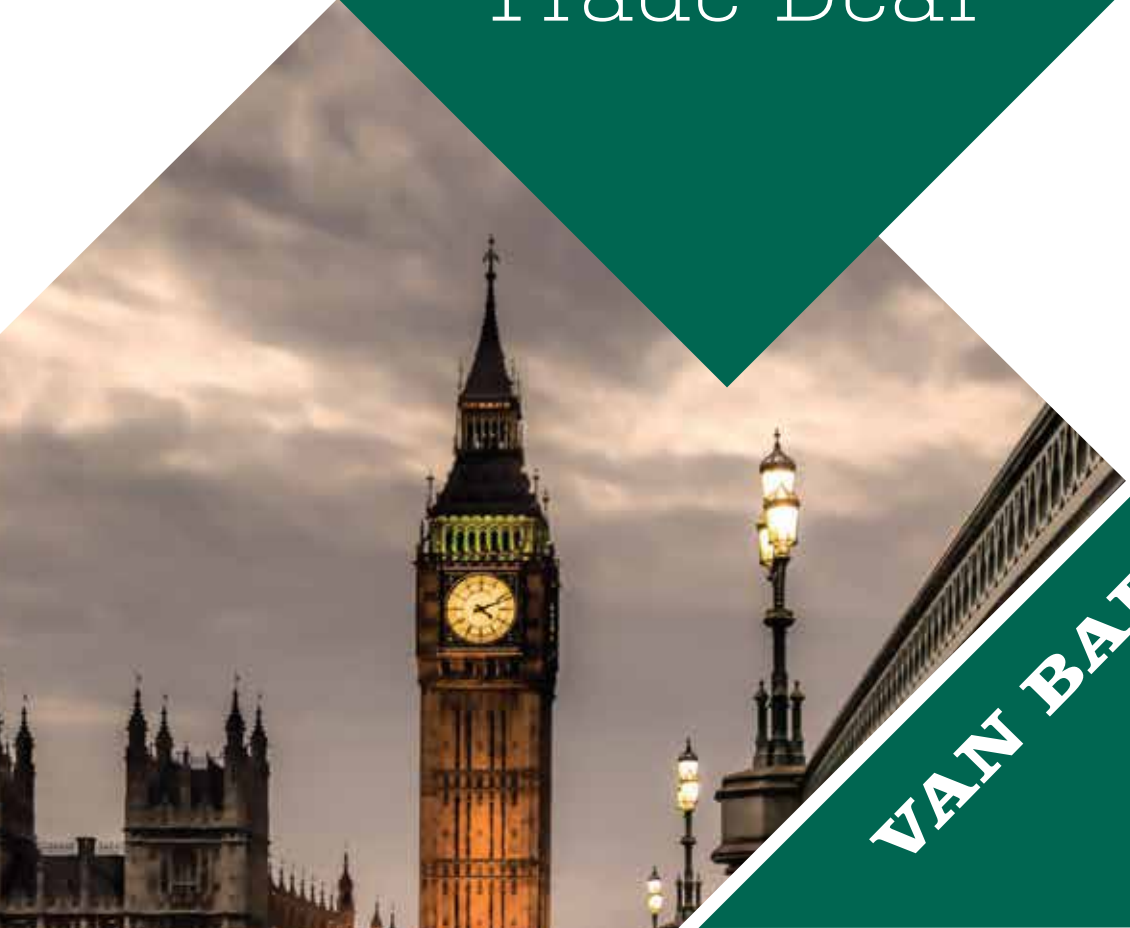
Brexit Implications for Data Protection in 8 Questions | Q&A Update under Brexit Trade Deal



VAN BAEL & BELLIS

Brexit Implications for Data Protection in 8 Questions | Q&A Update under Brexit Trade Deal.[1]

When the UK left the EU on 31 January 2020, the parties entered a transition period to negotiate a new relationship with the EU. On 24 December 2020, the UK and the EU agreed a Trade and Cooperation Agreement (***TCA***) regulating relations between both parties after Brexit. The TCA covers several topics, including data protection.[2]

Meanwhile, Brexit continues to raise many legal questions and uncertainties, not least as regards protecting personal data that flows between the UK and the rest of Europe. Will organisations in the UK still have to comply with the General Data Protection Regulation (***GDPR***)?[3] Can they still transfer personal data to the European Economic Area (***EEA***)[4] ? Will they need to appoint a representative in the EU? And what will happen with the "one-stop-shop"?

Based on eight frequently asked questions, we provide an overview of issues to consider and steps to take to be compliant with data protection rules in the EEA and the UK.[5]

1 Updated version as of February 2021.
2 Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part. Available here.
3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
4 The EEA includes the EU countries and Iceland, Liechtenstein, and Norway.
5 Please note that this Q&A should not be construed as legal advice on any specific facts or circumstances. The content is intended for general information purposes only. Readers should consult lawyers at the firm concerning any specific legal questions or the relevance of the subjects discussed herein to particular factual circumstances.

VAN BAEL & BELLIS

Chaussée de La Hulpe 166
B-1170 Brussels – Belgium

Phone : +32 (0)2 647 73 50
Fax : +32 (0)2 640 64 99

vbb@vbb.com
www.vbb.com

1 | WILL THE GDPR CONTINUE TO APPLY AFTER BREXIT?

Under the Withdrawal Agreement, concluded between the UK and the EU, the UK became a third country on 1 February 2020.[6] The Withdrawal Agreement provided for a transition period until 31 December 2020.[7] The UK was bound by EU law until that date, even though it was no longer represented in the EU institutions.

For any organisation that has an establishment in the EEA (i.e., the EEA without the UK), that organisation will have to continue to comply with the GDPR for all activities in the context of such establishment.

However, the GDPR may also continue to apply to organisations which are not (or are no longer) established in the EEA. This is because the GDPR, in any case, applies extraterritorially to the processing of personal data in order to "target" individuals in the EEA by: (i) offering goods or services to individuals in the EEA ("targeting by selling"); or (ii) monitoring the behaviour of individuals in the EEA ("targeting by monitoring").

The latter implies that the controller (i.e., the organisation that determines the purpose and means for the processing) has a specific purpose in mind for the collection and subsequent reuse of the relevant data about an individual's behaviour within the EEA (e.g., behavioural advertisements or online tracking through the use of cookies).

Moreover, the UK has adopted its own version of the GDPR (the so-called ***UK GDPR***)[8] to accommodate domestic areas of law, which entered into force on 31 December 2020.[9] From 1 January 2021, the UK GDPR together with the amended UK Data Protection Act 2018 and Privacy and Electronic Communications establish the personal data legislation in the UK. Therefore, the core data protection obligations remain very similar after Brexit for organisations based in the UK (however, see Question 7).

6 Article 185 of the Agreement on the Withdrawal of the United Kingdom from the European Union, published on 17 October 2019, available here.
7 Article 126 of the Agreement on the Withdrawal of the United Kingdom from the European Union, published on 17 October 2019, available here.
8 The draft Data Protection, Privacy and Electronic Communications (Amendment etc.) (EU Exit) Regulations 2019 is available here.
9 The UK GDPR was drafted from the EU GDPR text and revised so as to read the UK instead of the Union and domestic law rather than EU law.

2 | WILL I BE ALLOWED TO CONTINUE TRANSFERRING PERSONAL DATA FROM THE EEA TO THE UK AND VICE VERSA?

The TCA provides a temporary exemption for cross-border flows of personal data between the EEA and the UK. Those transfers will not be considered as data flows to a third country under the terms of the GDPR for a period of six months.[10] During this period, transfers of personal data between the EEA and the UK can continue without any additional safeguards being required. The six-month period could end earlier if an adequacy decision is adopted.

In a political declaration accompanying the TCA, the EU declares its intention to launch a procedure for the adoption of an adequacy decision with respect to the UK. With such a decision, the European Commission confirms that a third country's legislation provides an adequate level of protection for personal data and, as a result, personal data can be sent to that country without any further safeguards. It remains to be seen whether the European Commission will adopt an adequacy decision within this period.

If no adequacy decision is reached within the six-month period, rules on the international transfer of personal data to third countries will apply to data transfers to the UK. Therefore, organisations should prepare for this scenario and consider implementing appropriate safeguards.

For most organisations, these appropriate safeguards will take the form of Standard Contractual Clauses (***SCCs***). The SCCs are contractual arrangements that offer adequate safeguards with respect to the protection of personal data when these data are transferred to a third country.[11] Alternatively, some organisations may wish to rely on Binding Corporate Rules (***BCRs***) that authorise international transfers within the same group of companies. BCRs are binding policies on the protection of personal data that must be approved by the data protection authority of the company's lead supervisory authority. The approval process usually takes several months, so BCRs may not provide a short-term solution if the approval process has not yet been initiated. In addition, if you already have BCRs in place, these will need to be updated to recognise the UK as a third country. A third alternative provided by the GDPR is to adhere to codes of conduct that are approved by the European Data Protection Board (***EDPB***) or adhere to other clauses that would be approved. However, such measures are currently not yet available and will not provide a short-term solution either.

10 Article FINPROV.10A of the TCA.
11 Please note that the validity of the SCCs is currently under review by the Court of Justice of the EU. This will need to be considered when opting for the appropriate transfer mechanism.

Only in cases of exceptional circumstances and if the transfer is not structural, massive or repeated, can you transfer personal data outside the EEA without any of the above-mentioned safeguards. In such specific or exceptional situations, international transfers may be permitted on the basis of a data subject's informed and explicit consent, if it is necessary to defend a legal claim, or on the basis of other derogations set out in Article 49 of the GDPR.

For data transfers from the UK to the EU, the UK Government has proposed that, after Brexit, such data transfers will not be restricted. They will instead be covered by transitional provisions pending a UK adequacy decision.[12] If such transitional measures were repealed without an adequacy decision having been taken, the UK GDPR will require similar safeguards as set out above, namely ....

3 | WILL I HAVE TO APPOINT A EUROPEAN OR UK REPRESENTATIVE?

If you are based outside the EEA (and do not have any offices, branches or other establishments in the EEA) the GDPR may nevertheless still apply to your organisation if you "target" data subjects in the EU (see Question 1). In such a case, the GDPR requires that a representative within the EEA is designated. Consequently, UK-based organisations will, therefore, have to appoint an EU representative. The representative – set up in the Member State (or one of the Member States) where the data subjects that are monitored, or to whom goods or services are offered, are located – acts on behalf of the controller or processor with regard to their obligations under the GDPR and is the direct point of contact for data subjects and the competent authorities. You must provide the data subjects with the representative's details, which are usually mentioned in the privacy notice.

EXCEPTION: The requirement to appoint a representative does not apply to: (i) public authorities; and (ii) occasional processing activities with a low risk for the protection of rights and freedoms of individuals which does not involve the large-scale use of special category or criminal offence data.

Under the UK GDPR, the UK Government requires a controller or processor not established in the UK to appoint a UK representative under the same conditions as described above.

As a result, organisations outside the EEA that target data subjects in both the EEA and the UK will need an EU Representative as well as a UK representative.

12 Schedule 21, "Further transitional provision etc" of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

4 | I AM BASED IN THE UK BUT HAVE OFFICES, BRANCHES OR OTHER ESTABLISHMENTS IN THE EU: WHO WILL BE MY LEAD SUPERVISORY AUTHORITY?

The GDPR introduced a "one-stop-shop" mechanism, meaning that, in principle, a company only has to deal with one (single) lead supervisory authority if it is carrying out cross-border personal data processing activities. This mechanism thus establishes a single point of contact and precludes your organisation having to deal with questions from multiple authorities in parallel. The lead supervisory authority acts on behalf of the other EU supervisory authorities and is responsible for regulating your cross-border processing and for enforcing the GDPR (including by issuing fines).

Since the transition period has ended, the UK's Information Commissioner's Office (***ICO***) is no longer a competent authority under the GDPR. Therefore, as an organisation, you should consider whether you can still benefit from a lead supervisory authority in the EU. If the ICO is currently your lead supervisory authority, you may be advised to designate a new lead supervisory authority. The lead supervisory authority is the authority of the Member State where the organisation's main establishment or single establishment in the EU is located. To benefit from the "one-stop-shop", the decision making on the protection of personal data must be transferred to the location of the "main" establishment in the EU.[13]

5 | DO I NEED TO APPOINT A NEW DATA PROTECTION OFFICER?

The DPO

Some data controllers and data processors are required by the GDPR to designate a Data Protection Officer (*DPO*). This obligation applies if: (i) you are a public authority or body; (ii) your core activities require large scale, regular and systematic monitoring of individuals; or (iii) your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences. Groups of undertakings can designate one DPO for the entire group, provided that the DPO is easily accessible from every establishment and for all the data subjects concerned.

Even though the GDPR does not require the DPO to be located within the EU, the Article 29 Working Party recommends this, whether or not the controller or the processor is established in the EU. If you have currently appointed a DPO in the UK for a group of undertakings, the same person can continue to act as DPO after Brexit. However, you should assess whether the DPO is easily accessible from the EU.

13 Businesses that currently have the ICO as their lead authority, and which will continue to engage in cross-border processing within the EU, would be well advised, if they have not already done so, to start identifying whether they will then qualify as having an alternative "main" establishment within the remaining EU Member States.

6 | WHERE DO I NOTIFY DATA BREACHES AFTER BREXIT?

Under the GDPR, the controller must notify personal data breaches to the supervisory authority without undue delay and within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the breach is likely to result, however, in a high risk of adversely affecting individuals' rights and freedoms, you must not only notify the supervisory authority, but also inform those individuals affected by the breach without undue delay. Consequently, some UK organisations may still be subject to the GDPR if they have an establishment in the EEA or target EEA data subjects (see Question 1). The duty to notify personal data breaches under the GDPR may, therefore, still apply to you.

It is important to consider which supervisory authority must be notified. This will depend on whether the UK organisation has an establishment in the EEA or not. If you have an EEA establishment, any local breaches must be notified to the local supervisory authority, while breaches of a cross-border processing must only be notified to your lead supervisory authority, i.e., the authority of the Member State where you have your single or main EU establishment. If you do not have an EU establishment, you should notify cross-border breaches to the supervisory authority of the Member State where your EU representative is located (see Question 3).

Under the UK GDPR, EEA companies will have a similar duty, subject to the same conditions, to notify personal data breaches to the ICO.

CYBER SECURITY

How Will I Protect Network and Information Systems After Brexit?

The *Directive concerning measures for a high common level of security of network and information systems across the Union* (*NIS Directive*) creates common standards on network and information security across the EEA for "*operators of essential services*" (i.e., operators in the health, water, energy, transport, digital and financial sectors) and for "*digital service providers*" (i.e., online marketplaces, search engines and cloud computing services).[14] As it is a Directive, the national laws implementing the NIS Directive continue to apply in the UK after Brexit.

14 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, *EU OJ* L 194, p. 1. This Directive has been transposed into UK law by the NIS Regulations (SI 2018/506).

The NIS Directive requires digital service providers not established in the EEA to appoint an EU representative in the Member State (or one of the Member States) where their services are offered. To determine whether you provide services in the EEA that fall under the NIS Directive, factors such as the use of a language or currency generally used in a Member State or the mentioning of customers or users located in the EEA will play a role, among other factors. You will need to comply with the domestic legislation implementing the NIS Directive in that Member State where services are offered.

The NIS Directive imposes obligations with regard to preventive network and information security requirements. In addition, organisations within the material scope of the NIS rules must notify incidents with a substantial impact on the provision of services to the national authorities of that Member State. If the incident also relates to personal data, the notification under the NIS Directive is in addition to the data breach notification obligation under the GDPR. Accordingly, organisations should ensure that their incident response plans provide clear triggers to notify all relevant authorities in case of a breach.

7 | WILL THE PROTECTION OFFERED BY THE EU AND UK DATA PROTECTION RULES REMAIN THE SAME?

The UK has passed its own version of the GDPR into UK law, resulting in a "UK GDPR". The regulatory regimes for personal data protection, therefore, for the moment remain the same. However, the rules may diverge over time, either because the EU or UK amends its data protection rules, or as a consequence of UK regulators no longer being bound by interpretations of the Court of Justice of the EU (***CJEU***) or the European Data Protection Board (***EDPB***). Indeed, escaping the CJEU's jurisdiction is one of the reasons why the UK wishes to leave the EU. From now on, the UK Supreme Court will be the ultimate interpreter of the UK GDPR, and the ICO will publish its own guidance on the interpretation and application of data protection rules in the UK.

It is, therefore, possible that, after some time, equivalent rules might be applied differently depending on their interpretation in the EU or the UK. Such differences may also be relevant if the UK were to receive an adequacy decision of the European Commission (see Question 2), as this decision would need to be reviewed on a regular basis. Such review will look at possible divergences between EU and UK data protection rules. If the divergence were to become significant, the adequacy decision might be revoked.

8 | SHOULD I START PREPARING NOW ?

The above questions show that Brexit is likely to raise some data protection issues. As Brexit has dominated news headlines over the past few years, some organisations have already taken steps to prepare for Brexit, on the assumption that a TCA between the EU and the UK would not be reached.

Other organisations will be expected to act in line with the TCA. The GDPR already requires organisations to be "accountable" and accountability includes having a clear plan for protecting personal data after Brexit. Below, we provide an outline of what such a plan should cover.

TO DO:

First, start mapping your data flows (if any) between the EEA and the UK and have a clear view of contracts relating to such data flows. Mapping data flows may take some time, so it should not be left until the last minute.

Second, set out your strategy for international transfers outside the EEA: do you opt for SCCs or BCRs? In the latter case, you may already have to start implementing the BCRs.

Third, review your current contracts, including data processing agreements, general terms and conditions and other contracts with data protection clauses. The wording of these clauses may need to be updated to reflect the new situation after Brexit. For instance, if your contract asserts that personal data will not be transferred outside the EU, but you store data in the UK, you may need to amend the agreement or change your data storage location. In addition, some organisations may no longer wish to warrant that they will comply with EU law (including the GDPR) if this is no longer applicable to them.

Fourth, update your compliance documentation: privacy notices, breach notification procedures, Data Protection Impact Assessments (*DPIAs*) or other documentation. Policies should be updated to add a reference to "the EEA and the UK" since, in any case, the UK will no longer be part of the EU. In addition, DPIAs may need to be updated to describe international transfers and describe the strategy for dealing with such transfers.

Fifth, as a UK organisation, you should consider whether you should establish a branch office or affiliate in the EU, or transfer decisional powers to such an establishment, in order to benefit from the "one-stop-shop".

Sixth, make sure your appointed DPO in the UK for a group of undertakings is easily accessible from the EU.

Finally, determine whether an EU and/or UK representative needs to be appointed. You must provide the data subjects with the identity and contact details of the representative; this is usually done in the privacy notice.